Acceptable Use Standard

Purpose

The purpose of this standard is to outline the acceptable use of Whitworth University's computer equipment. An acceptable use standard is not written to impose restrictions that are contrary to Whitworth University's established culture of openness, trust and integrity.

Acceptable use supports our information assurance program and protects our Whitworth University system and partners from damaging actions. Inappropriate use exposes Whitworth University to risks that include malicious software attack, the compromise of network systems and services, and legal action.

Special Instructions

Effective security is a team effort involving the participation and support of every Whitworth University employee and affiliate who deals with information and/or Information Technology. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

When using personal computers, such as personal student computers, this Standard only applies to Whitworth University and network. For example, it would not be permitted for a student to send any confidential, inappropriate, offensive, illegal or any other class of unauthorized information over university equipment; including but not limited to the network managed by the university.

Applicability

This standard applies to employees, non-employee faculty, business partners, contractors, volunteers, student employees, and trainees. Third parties with access to Whitworth University's systems or data are also accountable for compliance with this standard. The use of the word "Users" in this manual includes all the above listed people.

General Use and Ownership

1. While Whitworth University's network will provide a reasonable level of privacy, communications or stored data may be subject to monitoring, interception and search, and may be disclosed or used for Whitworth University's interests. This privacy does not constitute consent for user misconduct and Whitworth University may audit networks and systems on a periodic or ongoing basis to ensure compliance with this standard.
2. Users should be aware that the data they create on company systems remains the property of Whitworth University. Trade secrets, operational details, and any work product shall remain the exclusive property of Whitworth University and must not be shared with anyone not previously authorized to receive such information (authorization MUST be in writing by a person duly authorized to provide

authorization). Whitworth University's Information Technology staff reserves the right to track or otherwise investigate user acceptable and unacceptable use.

3. Upon termination, graduation, expulsion, or otherwise leaving, users no longer have any rights to Whitworth University's data, intellectual property, trade secrets, operational processes, property or systems beyond that of a member of the public. Maintaining access to any Whitworth University's property or data may be construed as theft. Accessing any system in any manner inconsistent with that of the public will be construed as unauthorized access. Whitworth University reserves the right to report suspected crimes to the appropriate authorities.
4. Users are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for managing personal use details not addressed in this standard document. Users should consult their supervisor or manager in the absence of department direction.
5. Personally Identifiable Information (PII), Sensitive student information, or credit card communications will be encrypted if sent outside of Whitworth University's network (e.g., email, compact disc, flash memory storage device, etc.). Text messaging of any personally identifiable information shall be done, only with approval from the Information Assurance Team or Senior Management and in accordance with Whitworth University's Security Manual.
6. Users will immediately report all real or suspected security incidents immediately, including PII, or sensitive student information to their immediate supervisor or a member of the faculty or the Information Assurance Team. Faculty members will report the information to the IT Department immediately. This includes any item that is lost (or cannot be found after a reasonable attempt to locate it) that contains confidential information.
7. Users using workstations shall consider the sensitivity of the information, including sensitive student information that may be accessed, and minimize the possibility of unauthorized access.
8. Users will not access, store, process, display, distribute, transmit, or view material that is abusive, harassing, defamatory, vulgar, pornographic, profane or racist, that promotes hate crimes or is subversive or objectionable by nature, that encourages criminal activity, or violates local, state, federal or international law.
9. Users may use only employer provided software on their company provided computers and electronic devices. Downloading and/or installing any software shall be done with the approval of the IT Department.
10. All details of this standard apply to social networking that affects students or users, regardless of where the networking is performed.
11. Whitworth University's users will maintain physical and technical safeguards, for all workstations, devices, and confidential/proprietary information.
    a) **Appropriate physical measures include**:
        i) Safeguarding information and Information Technology from unauthorized or inadvertent modification, disclosure, destruction or misuse.

ii) Securing laptops and all portable devices and confidential information that contain sensitive information by using cable locks or by locking devices/information in drawers, offices, or cabinets.

iii) When off-site, computers and other portable devices, access documents, and any confidential or proprietary documents must be locked/secured in a manner that properly protects them from theft. When left in vehicles, every attempt should be used to hide these devices. When in public areas, such as airports, devices and confidential data should never be left unattended. Passwords and other access devices should never be stored with any portable device including writing them on anything.

iv) Reporting any known or suspected computer virus or malware behaviors. Indicators of malware include:

(1) Computer acting differently,

(2) Pop-up screens,

(3) Unexpected computer crashes,

(4) Strange windows opening

(5) Antivirus software disabled,

(6) Missing or moved items,

(7) Slow system

(8) Hard drive light on, all the time (the hard drive is running more than normal)

(9) Programs run, without interaction from you,

v) Ensuring that monitors are positioned away from public view or installing privacy screen filters or other physical barriers to public viewing.

vi) Not connecting any computing device to a Whitworth University's workstation or network, except as authorized by the CIO.

vii) Appropriately challenging or reporting any person or persons in non-public areas of the company or accessing any Whitworth University's equipment; who appear to or are known to be unauthorized.

viii) Clean/clear desk and clean/clear desk requirements;

(1) When your screen is not directly visible by you, lock the screen by holding the "Windows" key and the "L" and ensure that the screen locks.

(2) When leaving the area for more than 10 (ten) minutes, place all confidential/proprietary data into a locked drawer, file cabinet, etc. Ensure that the keys are not left in a manner that would permit access to these areas. This does not apply to locked offices.

(3) Ensure that confidential/proprietary data is not placed into trash cans, they are placed into the shred bins. At the end of the day, ensure that all

material designated to be shredded is placed into the shred bin, before going home.

b) Appropriate technical measures include:

i) Securing workstation displays (screen lock or logout) prior to leaving the immediate area.

ii) Closing all applications and documents before leaving the workstation for periods exceeding two hours.

iii) Ensuring passwords conform to Whitworth University's password standards and are never written or otherwise publicly displayed.

iv) Never installing or storing unauthorized software on company computers or the network.

v) Ensuring all workstation stored data (i.e., "data at rest") is encrypted.

vi) Ensuring all mobile device (e.g., USB drive, "thumb drive", CD/DVD, etc.) Non-Public data are encrypted.

vii) All company owned laptop computer hard drives should be encrypted.

viii) Ensuring workstations are left powered on but logged off to facilitate after hours' updates.

ix) If wireless network access is used, ensure access is secure by following the Wireless and Remote Access policy.

x) Information Technology department staff ensuring no sensitive Information exists on computer media or equipment before reuse or disposal.

Physical Security and Proprietary Information

1) Users will take all reasonable precautions to prevent unauthorized access to company private information, corporate strategies, competitor sensitive, trade secrets, specifications, student lists, and research data. Unauthorized access includes accessing any information not required to perform official duties, including but not limited to student data, and personnel and pay records.

2) Users will keep all access privileges physically secure and will not share individual accounts, accesses or passwords. Authorized users are responsible for the security of their passwords and accounts.

3) All user-used computers that are connected to Whitworth University's network, whether user or company owned, will be continually executing virus scanning and anti-spyware software with current signatures files. The owners of these computers will not store confidential data on these computers unless they are appropriately encrypted, and all software is up to date.

i) Portable devices (personal or otherwise) will be encrypted, if confidential data is stored, processed, or transmitted to or from the computers.

(1) Non-Whitworth University's systems that store, process or transmit Whitworth University's Confidential data shall be approved by the CIO or his/her designee, prior to allowing the data to be stored, processed, or transmitted to or from these devices.

ii) Users will virus-check all information before introducing or uploading it to Whitworth University's network. Additionally, these devices will run personal firewall software, unless the device operating system does not support such.

4) Users should not open emails received from unknown senders and should report these emails to Whitworth University's Help Desk.

5) Emails or telephone that direct a user to wire or transfer money, perform in a manner that inconsistent with normal practices, or anything that appears to be outside of norms MUST be verified by calling the person via a known good telephone number.

6) Users will not store company based PII or other confidential data or student data on personal removable computing devices without prior approval from the Information Assurance Team or CIO.

7) Users will pick up printed material in a timely manner from shared printers, fax machines, and other open areas of the company, and ensure sensitive information printed materials are kept secure.

8) Users will not violate the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations. This includes the use of personal equipment connected to university systems.

9) Users will not connect any personal devices to the network, without prior approval from the CIO.

10) Users will not export software, technical information, encryption software or technology, in violation of international or regional export control laws.

11) Users will not take any Whitworth University owned equipment, systems, data, or anything they are not specifically authorized to take offsite to any location that is not specifically authorized by the Director of Security.

Passwords/access

1. Passwords to all systems will be changed at least every 120 days or upon suspicion that a password has been compromised.

   i Administrators are encouraged to use a more secure Ninety (90) day expiration period.

2. Passwords will not be shared with others and accounts will not be shared, including with family and other household members.

3. Users will not provide access to any Whitworth University's system or data to any non-Whitworth University's user, including family members, without approval by the Information Assurance Team or CIO.

4. Information Technology department personnel will lock accounts not accessed over a 60-day period.
5. Users at Whitworth University MUST construct the passwords to their accounts (user IDs) that are not easily guessed or predictable. REQUIRED behaviors are:
    i Construct passwords with a minimum length of 8 characters, and include at least one alphabetic and one numeric character
    ii Do not construct passwords using dictionary words, names or parts of names, phone numbers, dates etc.
    iii Do not make passwords the same as user ID
    iv "PIN" style passwords should follow the same standards, where allowed and should be as complex (in accordance with this section) as allowed.
    v Do not construct passwords using Social Security numbers or any derivatives of (e.g., partial or scrambled Social Security numbers)
    vi Do not make passwords on production systems the same as those used to access systems in non-production environments.
    vii Where possible, passphrases should be used, instead of passwords.
        1 Passphrases are sentences with proper grammar and punctuation.

Email

1. Users will not send unsolicited mass-recipient email messages (spam) or other advertising to individuals who did not specifically request such.
2. Users will not use email to harass, through message language, frequency, or size.
3. Users will only use email header information for official purposes and not solicit address information with the intent to harass or to collect replies.
4. Email will not be used to create or forward chain-letter email.
5. The use of email to facilitate private commercial business is not acceptable.

Internet Presence

1. Recognizing that internet-based activity can directly impact user productivity, all users will refer to the rest of this standard for guidelines on personal use and will consult with their managers for more information.
2. The use of the Internet to facilitate private (non-Whitworth University) commercial business is not acceptable unless otherwise specifically authorized.
3. Limited and occasional use of Whitworth University's systems to engage in personal activities is acceptable if it is done in a professional and responsible manner, does not otherwise violate Whitworth University

standards of conduct, and is not detrimental to Whitworth University's best interests.

4. Users will not post any information concerning confidential or proprietary information the operations of Whitworth University to any public website.
5. Users will not engage in any blogging that may harm or tarnish the image, reputation or goodwill of Whitworth University, or any of its users. Users are prohibited from making any discriminatory, disparaging, defamatory or harassing comments or creating a hostile environment through the use of technology.
6. Users MUST NOT attribute personal statements, opinions or beliefs to Whitworth University or opinions in blog, the user may not, expressly or implicitly, represent themselves as an user or representative of Whitworth University Users will not use any Whitworth University's systems to perform any of these activities. Users assume all risk associated with blogging.
7. Apart from following all laws pertaining to the handling and disclosure of copyrighted or export-controlled materials, Whitworth University's trademarks, logos and any other Whitworth University's intellectual property may not be used about any blogging activity, except as approved by University Cabinet/executive leadership team.
8. Users will not post to newsgroups with their Whitworth University email address, unless such posting is during business duties.

Unacceptable Use

The following activities provide a framework for activities which fall into the category of unacceptable use and are, in general, prohibited. Users may be exempted from these restrictions while performing legitimate job responsibilities.

1. The storage, installation or distribution of unauthorized software or products not appropriately licensed for use by Whitworth University (this cannot be exempted if it violates any law or copyright requirement).
2. Introducing, coding, compiling, storing, transmitting or transferring malicious software code, including but not limited to viruses, worms and Trojan horses.
3. Uploading or downloading executable software (e.g., screensavers, entertainment software, games, etc.) without prior approval from the Information Assurance Team or CIO.
4. Gambling, wagering or placing any online bets.
5. Using a Whitworth University's computing asset to procure or transmit material that is in violation of sexual harassment, racism, sexism, or any

form of hostile workplace laws. This includes using personal equipment to violate sexual harassment or hostile workplace laws.

6. Making fraudulent offers of products, items, or services originating from any Whitworth University system or system account.
7. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or logging into a server or account that the user is not expressly authorized to access.
8. Relocating or changing equipment, or the network connectivity of the equipment, without prior authorization from the Information Assurance Team or CIO.
9. Network port scanning or security scanning without prior approval of the Information Assurance Team or CIO.
10. Executing any form of network monitoring which will intercept data not intended for the user's computer, without prior approval of the Information Assurance Team or CIO.
11. Circumventing user authentication or security of any host, network or account.
12. Interfering with or denying service to any authorized Whitworth University's user in support of their official duties.
13. Using any program, script, command, or sending messages of any kind, with the intent to interfere with or disable another user's session or account.
14. Providing information about or lists of Whitworth University's users to parties outside Whitworth University, except in support of their official duties.

Under no circumstances is a user of Whitworth University systems authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Whitworth University owned resources.

Users are accountable for compliance with all security policies and are required to read and understand them. Please note that user's responsibilities for protecting Whitworth University information do not end at termination of employment. These responsibilities continue until the information is reclassified to be public.